CLAIMS

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said one of the cryptographic operations comprises:

a plurality of OFB block cryptographic operations performed on a corresponding plurality of input text blocks;

OFB mode logic, operatively coupled to said cryptographic instruction, configured to direct said computing device to update pointer registers and an initialization vector location for each of said plurality of OFB block cryptographic operations; and

execution logic, operatively coupled to said OFB block pointer logic, configured to execute said one of the cryptographic operations.

2. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an OFB mode encryption operation, said OFB mode encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

3. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an OFB mode decryption operation, said OFB mode decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

4. The apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

5. The apparatus as recited in claim 1, wherein said cryptographic instruction prescribes that output feedback mode to be employed in accomplishing said one of the cryptographic operations.

6. The apparatus as recited in claim 1, further comprising:

a bit, coupled to said execution logic, configured to indicate whether said one of the cryptographic operations has been interrupted by an interrupting event.

7. The apparatus as recited in claim 6, wherein said bit is contained within a flags register.

8. The apparatus as recited in claim 6, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said one of the cryptographic operations on a current input text block is interrupted.

9. The apparatus as recited in claim 8, wherein, upon return of program control to said cryptographic instruction, said one of the cryptographic operations is performed on said current input text block.

10. The apparatus as recited in claim 1, wherein said OFB mode logic directs said computing device to modify said pointer registers to point to next input and output text blocks at the completion of each of said plurality of OFB block cryptographic operations on each of said corresponding plurality of input text blocks.

11. The apparatus as recited in claim 1, wherein said OFB mode logic directs said computing device to store a current initialization vector equivalent to a memory location pointed to by an initialization vector register.

12. The apparatus as recited in claim 11, wherein said OFB mode logic directs said computing device to generate said current initialization vector equivalent by exclusive-ORing a current input text block with a current output text block.

13. The apparatus as recited in claim 1, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

14. The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

15. The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said computing device.

16. The apparatus as recited in claim 15, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

17. The apparatus as recited in claim 15, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

18. The apparatus as recited in claim 15, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

19. The apparatus as recited in claim 15, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

20. The apparatus as recited in claim 15, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations.

21. The apparatus as recited in claim 15, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

22. The apparatus as recited in claim 1, wherein said execution logic comprises:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

23. An apparatus for performing cryptographic operations, comprising:

a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said one of the cryptographic operations comprises:

plurality of OFB block cryptographic operations performed on a corresponding plurality of input text blocks; and

OFB mode logic, operatively coupled to said cryptography unit, configured to direct said device to update pointer registers and contents of an initialization vector location for each of said plurality of OFB block cryptographic operations.

24. The apparatus as recited in claim 23, wherein an interrupting event causes a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said one of the cryptographic operations on a current input text block is interrupted.

25. The apparatus as recited in claim 24, wherein, upon return of program control to said cryptographic instruction, said one of the cryptographic operations is performed on said current input text block.

26. The apparatus as recited in claim 23, wherein said OFB mode logic directs said computing device to modify said pointer registers to point to next input and output text blocks at the completion of each of said plurality of OFB block cryptographic operations on each of said corresponding plurality of input text blocks.

27. The apparatus as recited in claim 23, wherein said OFB mode logic directs said computing device to store an initialization vector equivalent to said initialization vector location, wherein said initialization vector location comprises a memory location pointed to by an initialization vector register.

28. The apparatus as recited in claim 23, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

29. The apparatus as recited in claim 23, wherein said OFB mode logic directs said computing device to generate an initialization vector equivalent by exclusive-ORing a current input text block with a current output text block.

30. A method for performing cryptographic operations in a device, the method comprising:

executing one of the cryptographic operations responsive to receiving a cryptographic instruction, wherein the cryptographic instruction prescribes the one of the cryptographic operations, said executing comprising:

performing a plurality of OFB mode block operations on a corresponding plurality of input text blocks; and

writing an initialization vector equivalent to an initialization vector location for employment by a following one of the plurality of OFB mode block operations on a following one of the plurality of input text blocks.

31. The method as recited in claim 30, further comprising:

transferring program control to a program flow configured to process a interrupting event, and interrupting said executing of the one of the cryptographic operations on the current input text block.

32. The method as recited in claim 31, further comprising:

upon return of program control to the cryptographic instruction following said transferring, performing said executing on the current input text block.

33. The apparatus as recited in claim 30, wherein said receiving comprises:

prescribing the cryptographic instruction according to the x86 instruction format.

34. The method as recited in claim 30, wherein said receiving comprises:

prescribing an output feedback mode encryption operation as the one of the cryptographic operations.

35. The method as recited in claim 30, wherein said receiving comprises:

prescribing an output feedback mode decryption operation as the one of the cryptographic operations.

36. The method as recited in claim 30, wherein said executing comprises:

accomplishing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

37. The method as recited in claim 30, further comprising:

generating the initialization vector equivalent.

38. The method as recited in claim 37, wherein said generating comprises:

exclusive-ORing a current input text block with a current output text block.